Microsoft Sentinel and Defender XDR QuickStart

Reduce complexity, optimize costs, improve visibility and detection, and enhance automation and response capabilities with this accelerated program.

3-4 month SIEM engagement

Cyber threats are becoming more sophisticated, frequent, and targeted every day. Organizations are in a constant battle to protect their users, data, and assets from a variety of attacks. Unfortunately, traditional security tools and processes are often inadequate or siloed to enable a proper or effective response to such threats.

To combat this, MNP Digital's security experts have created a QuickStart to help you implement a Security Operations Center (SOC) built on Microsoft Security solutions, incorporating Microsoft Sentinel as the cloud-native SIEM solution and Microsoft Defender XDR. Both solutions leverage artificial intelligence and provide automation capabilities, offering unified visibility, more accurate threat detection, and stronger response capabilities.

MNP Digital also offers a fully managed approach to the implementation of SOC services, providing you with ongoing optimized protection. Learn how our experts can help you move forward with confidence.

Expected outcomes

- Security operations center (SOC) implemented with the cloud-native Microsoft Sentinel solution
- Enabled built-in orchestration automation and response capabilities
- Enhanced benefits and efficiencies via MNP's Managed Security services
- Partnership with a Canadian-staffed and security-cleared SOC
- Extended 24x7 incident management support

Microsoft Partner

What's included

To be tailored to your organization's needs.

	1. Discover / Deploy	Optional add-on engagements 2. Tune	3. Detect & Respond
Objectives	• Capture business requirements and understand network topology and data flows • Maximize overall threat monitoring and detection coverage	• Conduct reviews with the security team and ensure regular processes and reports are developed • Ensure alerts/call escalation procedures are completed	• Prepare documentation and training materials • Recommend tools and services to extend security visibility • Leverage orchestration and automation
Activities	• 1-hour complementary intro session • Validate the state of the existing environment • Deploy Microsoft Sentinel as the cloud-native SIEM solution • Deploy virtual log collectors for on-prem infrastructure and built-in connectors for cloud-based applications	• Establish customized dashboard views • Integrate additional third-party systems and applications with Microsoft Sentinel • Ensure accurate event and log ingestion • Complete any cloud or SaaS-based application connectors	• Document and implement security automation workflows • *Optional - Finalize and formalize your response plan with MNP's Incident Response Team* • *Optional - Perform tabletop exercises with executives*
Deliverables	• Proof of value documentation • Functional Microsoft Sentinel platform with knowledge transfer sessions • Review critical and high detections over a two-week deployment period	• Finalize dashboard and reporting functionality • Complete log tuning and filtering as appropriate • Provide on-going "as-built" documentation workbooks	• Review and triage any critical or high-risk findings • Implement security orchestration activities • Establish cadence of external vulnerability scanning and virtual CISO engagement
Timing	• 3-4 Months	• Ongoing (annual retainer)	• Ongoing (annual retainer)

MNP DIGITAL

Our scalable team of expert advisors, problem solvers, and builders ensure you receive the specific skills and guidance you need to get the most out of your digital investments.

Want to learn more? Visit **mnpdigital.ca**

Ready to get started?

Ahmed Otmani Amaoui
Partner, Microsoft Lead
416.991.2748

ahmed.otmani@mnp.ca

Microsoft Partner